STATE OF ALABAMA

Information Technology Standard

Standard 680-01S2: Protecting Personally Identifiable Information (PII)

1. INTRODUCTION:

This standard establishes requirements for the protection of electronic records containing Personally Identifiable Information (PII) that is either accessed remotely or physically transported or stored on mobile devices.

2. OBJECTIVE:

Protect PII electronic records from unauthorized modification, disclosure, or loss.

3. SCOPE:

These requirements apply to all State-owned or controlled information systems or services that receive, process, store, display or transmit State information regardless of classification or sensitivity (includes contracted or outsourced access to State information and resources).

4. REQUIREMENTS:

4.1 CONFIRM PII PROTECTION NEEDS

Ensure information system owners and data owners identify PII, evaluate the risk of loss or unauthorized disclosure, and establish required access controls for PII in other media.

All PII not explicitly cleared for public release shall be protected in accordance with information protection category Sensitive, as established in State standards with additional protections as required by this standard and organizational procedures.

All PII shall be evaluated for impact of loss or unauthorized modification or disclosure and protected accordingly. Additionally, all State of Alabama information system and data owners shall conduct risk assessments of compilations of PII and identify those needing more stringent protection (such as for remote access or mobile computing).

4.2 PII TRANSPORTED/STORED OFF-SITE

Electronic PII records shall not be routinely processed or stored on mobile computing devices or removable electronic media without express approval of the data owner.

Except for compelling operational needs, any mobile computing device or removable electronic media that processes or stores electronic PII records shall be restricted to workplaces that minimally satisfy State standards for physical and environmental security (hereinafter referred to as “protected workplaces”).

Any mobile computing device containing electronic PII records removed from protected workplaces, including those approved for routine processing, shall:

- Be signed in and out with a supervising official designated in writing by the organization Information Security Officer (ISO) or agency head.
- Require certificate based authentication using a State or State-approved PKI certificate on an approved hardware token to access the device.
- Implement a screen lock control with a specified period of inactivity not to exceed 15 minutes.
- Encrypt all data at rest, i.e., all hard drives or other storage media within the device as well as all removable media created by or written from the device. Encryption shall comply with State standards.

4.3 PII REMOTE ACCESS PROTECTIONS

Remote access to PII records is permitted only for compelling operational needs, and:

- Shall employ certificate based authentication using a State or State-approved PKI certificate on an approved hardware token.
- Any remote device gaining access shall implement a screen lock control with a specified period of inactivity not to exceed 15 minutes.
- No information, including encrypted representations of information, produced by a prior subject's actions is available to any subject that obtains access to an object that has been released back to the system (i.e., absolutely no residual data from the former object).
- Download and local/remote storage of PII records is prohibited except as described in section 4.2 of this standard and only if expressly approved by the data owner.

Only State authorized devices shall be used for remote access. All remote access shall comply with applicable State standards.

4.4 DATA LOSS PROCEDURES

The Information Security Officer (ISO) of the Information Services Division (ISD) of the Department of Finance, as the Senior ISO for the State of Alabama, shall establish procedures for reporting the compromise, loss, or suspected loss of PII within ISD, entities supported by ISD, and adoptable by all entities statewide.

Heads of State Entities shall:

In accordance with this standard and direction from the State Senior ISO, establish reporting procedures to ensure that compromise, loss, or suspected loss of PII is reported in accordance with State requirements.

Ensure supervising officials establish logging and tracking procedures for electronic PII records on mobile computing devices or portable media removed from protected workplaces.

5. DEFINITIONS:

INDIVIDUAL. A living person who is a citizen of the United States or an alien lawfully admitted for permanent residence. The parent of a minor or the legal guardian of any individual also may act on behalf of an individual. State of Alabama employees are "individuals." Corporations, partnerships, sole proprietorships, professional groups, businesses, whether incorporated or unincorporated, and other commercial entities, are not "individuals."

INDIVIDUAL IDENTIFIER. Information associated with a single individual and used to distinguish him or her from other individuals (e.g., name, Social Security number or other identifying number, symbol, or other identifying particular such as a finger or voice print or photograph).

IDENTIFYING INFORMATION. As defined in the Code of Alabama, Section 13A-8-191 (Act 2001-312, p. 399, §2.), any information, used either alone or in conjunction with other information that specifically identifies a person or a person's property, and includes, but is not limited to, any of the following information related to a person:

- Name
- Date of birth
- Social Security number
- Driver's license number
- Financial services account numbers, including checking and savings accounts
- Credit or debit card numbers
- Personal identification numbers (PIN)
- Electronic identification codes
- Automated or electronic signatures
- Biometric data
- Fingerprints
- Passwords
- Parent's legal surname prior to marriage
- Any other numbers or information that can be used to access a person's financial resources, obtain identification, act as identification, or obtain goods or services

PERSONALLY IDENTIFIABLE INFORMATION (PII). Any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, Social Security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.

PII ELECTRONIC RECORD. Any item, collection, or grouping of information in electronic form that associates personal information such as education, financial transactions, medical history, criminal or employment history, with an individual identifier. Also any item, collection, or grouping of information in electronic form that associates two or more individual identifiers (e.g., name and social security number). Electronic records that contain information about education, financial transactions, medical history, or criminal or employment history but do not include individual identifiers are not considered PII electronic records.

6. ADDITIONAL INFORMATION:

6.1 POLICY

Information Technology Policy 680-01: Information Protection

6.2 RELATED DOCUMENTS

Information Technology Standard 680-01S1: Information Protection

Information Technology Standard 650-01S1: Physical Security

Information Technology Procedure 600-04P1: Cyber Security Incident Reporting

Signed by Eugene J. Akers, Ph.D., Assistant Director

Revision History

Version	Release Date	Comments
Original	02/06/2007	